1. (**Currently Amended**) A method for generating an Identification and Verification Template (IVT) **for a biometric** comprising the steps of:

obtaining a user biometric from a biometric system **with one or more servers**, **wherein the biometric system includes one or more biometric scanners to collect physical information from the user which is stored as bits of information on the biometric system**, wherein~~,~~ the user biometric includes previously encoded authorization information defining a set of privileges granted to a user by an authorization officer for a security infrastructure; ~~and~~

generating a dependency vector from the user biometric **on an identification processing system with one or more servers**, wherein the dependency vector is generated with a lossy transformation of information stored in the user biometric; **and**

storing the dependency vector in an Identification and Verification Template (IVT) on a reliable storage medium **external to the identification processing system**, such that the IVT is bound cryptographically to ~~a~~ **the** user from which the user biometric was obtained, wherein the IVT does not include complete information from the obtained user biometric but does allow for verification of the user when the IVT is accessed for the security infrastructure at a later time.

2. (**Previously Presented**) The method of claim 1, wherein the dependency vector includes check digits of the user biometric generated using an error correcting code.



LESAVICH HIGH-TECH
LAW GROUP, P.C.
SUITE 325
39 SOUTH LASALLE STREET
CHICAGO, ILLINOIS 60603-1601
TELEPHONE (312) 332-3751

3. (**Previously Presented**) The method of claim 1, wherein a canonical user biometric is generated from a biometric processing function of multiple readings of the user biometric from the user.

4. (**Previously Presented**) The method of claim 3, wherein the biometric processing function is a majority decoding function.

5. (**Previously Presented**) The method of claim 1, in which the IVT includes public identification information for the user.

6. (**Currently Amended**) A method for uniquely identifying a user via biometric analysis comprising the steps of:

acquiring an input from a user comprising a User Biometric (UB) from an offline reader**, wherein the offline reader includes one or more scanners to acquire physical information about the user**;

acquiring an input comprising an Identification and Verification Template (IVT) from a token or card on an **identification processing system with one or more servers**, wherein



LESAVICH HIGH-TECH
LAW GROUP, P.C.
SUITE 325
39 SOUTH LASALLE STREET
CHICAGO, ILLINOIS 60603-1601
TELEPHONE (312) 332-3751

the IVT was generated by the **identification processing system** with a lossy transformation of a previously obtained UB, is cryptographically bound to a user from which the UB was obtained and wherein the IVT does not include complete information from the obtained UB but does allow for verification of the user when the IVT is accessed for a security infrastructure at a later **time**; and

performing a validation protocol **on the identification processing system** with the UB and the IVT, whereby a decision value is computed giving either Authorization privileges or Other privileges to the user for access to the security infrastructure, where Other privileges may be anything else but Authorization privileges, wherein the validation protocol does not require use of a compare operation between the acquired UB and the acquired IVT.

7. (**Previously Presented**) The method of claim 6, wherein the validation protocol is a cryptographic validation mechanism for an authentication scheme.

8. **(Previously Presented**) The method of claim 6, wherein the acquired UB is an iris scan or a portion of an iris scan of the user.

9. (**Previously Presented**) The method of claim 6, where the acquired UB is derived from a biometric processing function comprising multiple scans of the UB.



LESAVICH HIGH-TECH
LAW GROUP, P.C.
SUITE 325
39 SOUTH LASALLE STREET
CHICAGO, ILLINOIS 60603-1601
TELEPHONE (312) 332-3751

10. (**Previously Presented**) The method of claim 9, where the biometric processing function includes a majority decoding function.

11. (**Previously Presented**) The method of claim 10, where the biometric processing function further includes error correction of a biometric component after the majority decoding function is applied.

12. (**Previously Presented)** The method of claim 6, where the IVT incorporates a password encrypted value of the IVT.

13. (**Currently Amended**) A method of secure biometric pattern recognition comprising the steps of:

acquiring a first user biometric (UB) pattern **from a biometric system with one or more servers, wherein the biometric system includes one or more scanners to collect physical information from the user**;

acquiring authenticating information **from a reliable storage medium previously generated by an identification processing system with one or more servers, wherein the reliable storage medium is external to the identification processing system;**

combining the UB pattern with the authenticating information with a lossy transformation of information stored in the UB **on the identification processing system**;



LESAVICH HIGH-TECH
LAW GROUP, P.C.
SUITE 325
39 SOUTH LASALLE STREET
CHICAGO, ILLINOIS 60603-1601
TELEPHONE (312) 332-3751

encrypting the combination of the UB pattern and the authenticating information to provide an Identification and Verification Template (IVT), wherein the IVT includes less than all information obtained from the first UB;

acquiring a second UB pattern **from the biometric system**; and

processing the second UB pattern and the IVT **on the identification processing system** to determine if the first UB pattern and the second UB pattern are the same **without directly comparing the first UB pattern with the second UB pattern**.

14. (**Previously Presented**) The method of Claim 13 wherein the processing step does not require use of a compare operation between the acquired second UB pattern and the IVT to securely identified a user associated with the second UB.

15. **(Original**) The method of claim 1, wherein the user biometric is an iris scan or a portion of an iris scan of the user.

16. (**Original**) The method of claim 1, wherein the reliable storage medium includes a magnetic strip or smart card.



LESAVICH HIGH-TECH
LAW GROUP, P.C.
SUITE 325
39 SOUTH LASALLE STREET
CHICAGO, ILLINOIS 60603-1601
TELEPHONE (312) 332-3751